I. PURPOSE

To establish configuration standards for DPS systems and to establish information security guidelines for the use of these systems.

II. SCOPE

This policy applies to all employees, including permanent, contractual, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office.

Statutory and/or Regulatory Authority: Statewide Information Security Manual; §147-110

III. POLICY

1. Unless authorized by the CIO, all DPS systems shall be configured and maintained by authorized MIS personnel.

2. MIS shall establish a baseline image for all DPS systems. Configuration management processes will be followed for modifications to the baseline image. Significant modifications to the baseline image will be reviewed by the DPS Information Security Office. At a minimum, each baseline image shall incorporate the following:

   - Authentication/Logon requirement
   - 10 minute time-out interval[1]
   - Anti virus software
   - Sign-on warning banner when feasible

---

[1] Extension of the time out interval will be considered on a case-by-case basis as the need warrants. Examples considered include systems used **exclusively** for presentations, training, or displays.

	Division:	**ADMINISTRATION**
State of North Carolina **DPS**	Chapter:	**INFORMATION TECHNOLOGY**
Department of Public Safety *POLICIES & PROCEDURES*	Policy:	**DESKTOP/LAPTOP CONFIGURATION**
INFORMATION TECHNOLOGY	Section:	**PURPOSE, SCOPE, POLICY**
	Issue Date:	**JANUARY 26, 2013**
	Revised:	

3. Prior to reassignment of a DPS system, the system shall be wiped/re-imaged by authorized MIS personnel.